FTC Email Authentication Summit

Mike Chadwick
VP, Application Development
GoDaddy.com

November 9th, 2004

Who is GoDaddy.com?

- Main customers are small to medium size businesses and individual consumers, currently over 2 million customers use GoDaddy for their web presence needs.
- Medium size company (530 employees) focused on 100% customer satisfaction. Over 260 employees work in the customer contact center supporting our customers.

Who Is GoDaddy.com

Key Products

- Domain Names – Over 6 million domains under management and the #1 in net new growth monthly.
- Web site Hosting – Over 300,000 websites and one of the fastest growing in the shared hosting space.
- Email – Over 900k accounts and growing fast, over 300k separate domains used in the email system.
- SSL (Secure Certificates) – Fast growing Web Trust accredited Certificate Authority.
- DNS Services – Over 3 million domains use Go Daddy for DNS services.

Secondary Products

- Search Engine optimization
- Web site builders
- E-Commerce
- Email marketing
- Online Storage
- Copyright Registrations

GoDaddy.com's SMTP Implementation

- GoDaddy's SMTP system is made up of multiple filters to protect against spam and phishing.
  - SMTP Connection Blocking
    - Go Daddy maintains its own IP based whitelist and blacklist that determines if we accept a connection.
    - Go Daddy subscribes to the Bonded Sender whitelist.
  - We support SPF Classic in our SMTP system to perform email authentication.
  - Go Daddy also has a variety of custom built spam, virus, and anti-phishing filters to protect our customers.

Customer Implementation

- GoDaddy believes that customers need the ability to protect their domains easily.
  - Email Authentication isn't just for large corporations.
  - Must be easy for small businesses to protect their domains using email authentication standards.
  - Currently Go Daddy provides our customers with an easy to use interface for publishing SPF records for a domain.
  - Customers will need an easy way to protect their domain's reputation as reputation services become more prevalent.

Implementation Hurdles

- The current proposals do not contain centralized testing and validation.
  - Go Daddy had to help many companies fix their SPF records.
  - The customer impact of incorrect SPF records is significant as a lot of valid email can be rejected.
  - A training and validation process for an implementation needs to be considered as part of any proposal.
- Forwarding of emails
  - Go Daddy forwards millions of emails per day for customers, as do many of our competitors.
  - Forwarding is much more common than people think and the proposals need to take this into account.

Which Authentication Approach

- One email authentication standard is ideal and most practical.
  - The cost to implement for our own SMTP system 3-4 different approaches is prohibitive and overly complex.
  - Multiple approaches will cause confusion in the small to medium size business segment.
  - Multiple approaches will reduce the benefits of email authentication industry wide.
    - Most companies will only implement one or two for cost reasons.
    - Confusion will cause some smaller businesses and domain owners to not utilize any approach.
    - Competing standards may open up too many holes allowing spammers to continue to succeed.
- Go Daddy is committed to supporting any widely adopted approach.
- Go Daddy is working with Microsoft on Sender ID and will be an early implementer of the specification.

Implementation Statistics

- SMTP Implementation
  - Go Daddy currently blocks 70% of all connections using our blacklist.
  - IP based blacklisting must continue to exist to protect email systems from overload.
- SPF Implementation
  - 7% of all email coming into Go Daddy systems have SPF records associated with the domain. (~12 million emails per day)
  - 18% of email checked against SPF records are rejected.
  - 14% of the domains that pass SPF checks are known spammers.

Domain Reputation

- Any widely adopted approach needs domain reputation associated with it.
  - Spammers and phishers can easily utilize any of the proposed standards. They just need to buy a domain and publish their records.
  - 14% of SPF passed emails are already sent by spammers and this is increasing.
  - Reputation associated with a domain needs to be part of any standard to positively impact the amount of spam and phishing attacks.
  - Without reputation services of some sort we will have to continue providing multiple levels of filtering and blocking to combat spam and phishing attacks.